Συνοπτικός Οδηγός Θεμάτων Ασφάλειας της Πληροφορίας αλλά και των Προσωπικών Δεδομένων, για τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation 2016/679)

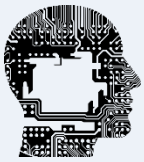
Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες ανθρώπινο δικαίωμα.

Ο κανονισμός (ΕΕ 2016/679) θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα ο κανονισμός παρέχει δικαιώματα στα φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προσωπικά δεδομένα (τους υπευθύνους επεξεργασίας).
eur-lex.europa.eu

Πεδίο Εφαρμογής

- επεξεργασία δεδομένων προσωπικού χαρακτήρα, σε σύστημα αρχειοθέτησης. [άρθρα 2,3]
- εντός Ευρωπαϊκής Ένωσης ή/και αφορά Ευρωπαίους πολίτες.

Δεδομένα Προσωπικού Χαρακτήρα



Οποιαδήποτε πληροφορία σχετική με την ταυτοποίηση ή την δυνάμει ταυτοποίηση φυσικού προσώπου συμπεριλαμβανομένων δεδομένων που καταγράφονται / χρησιμοποιούνται από υπολογιστές, κινητά, δίκτυα ή άλλες τεχνολογίες ειδικά όταν συνδυάζονται μαζί με άλλα δεδομένα. [άρθρο 4(1)]

Για παράδειγμα, Ονοματεπώνυμο, Διεύθυνση, Τηλέφωνο, Στοιχεία Πληρωμών, IP Address, Cookies, Email, Username, Password, Δεδομένα Θέσης, Website Session ID, RFI Tag, κ.α.

Ασφάλεια Επεξεργασίας

Ανά περίπτωση εφαρμόζονται κατάλληλα μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι κινδύνων, για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. [άρθρο 32]

Γνωστοποίηση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, επικοινωνούμε το περιστατικό στον Υπεύθυνο Ασφαλείας ή/και στον DPO.

Πολιτική Ασφαλείας Πληροφοριών

- Είναι ένα σύνολο κειμένων όπου αναφέρονται οι κρίσιμοι πληροφοριακοί πόροι της επιχείρησης και περιγράφονται οι τρόποι που αυτοί μπορούν και πρέπει να προστατευτούν. Για το σκοπό αυτό προσδιορίζονται διαδικασίες, οδηγίες και πρακτικές, οι οποίες διαμορφώνουν και διαχειρίζονται το ευρύτερο περιβάλλον ασφάλειας της επιχείρησης.
- Η πολιτική ασφάλειας εκφράζει την φιλοσοφία της επιχείρησης και τις απαιτήσεις για τη διασφάλιση των πληροφοριακών πόρων.

Ποιον σκοπό εξυπηρετεί;

- Προστατεύονται τα δεδομένα της επιχείρησης.
- Έχουν εντοπιστεί τρωτά σημεία στα πληροφοριακά συστήματα και με τις πολιτικές λαμβάνονται μέτρα για την κάλυψή τους. Έτσι κατοχυρώνεται η επιχειρησιακή συνέχεια και ενισχύεται η ασφάλεια της πληροφοριακή υποδομής.
- Ακολουθώντας την πολιτική ασφάλειας στις καθημερινές τους συναλλαγές με συναδέλφους, πελάτες και συνεργάτες, διασφαλίζεται ότι οι πληροφορίες ανταλλάσσονται με ασφαλή τρόπο και έτσι μειώνονται οι επιχειρησιακοί κίνδυνοι.
- Όταν υπάρχει και εφαρμόζεται η πολιτική ασφάλειας, κάθε εργαζόμενος αποκτά επίγνωση των κινδύνων αυξάνοντας έτσι την πιθανότητα συμμόρφωσής του με τους κανόνες της.

Η Ασφάλεια Πληροφοριακών Συστημάτων στηρίζεται σε τρεις βασικές αρχές.

Εμπιστευτικότητα (Confidentiality) - σημαίνει ότι πληροφορίες ή τα δεδομένα δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, δηλαδή με την κλοπή φορητών υπολογιστών από τμήμα μιας εταιρίας.

Ακεραιότητα (Integrity) - αναφέρεται στη διατήρηση των δεδομένων σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες αλλοιώσεις από μη εξουσιοδοτημένα άτομα.

Για παράδειγμα, το 1995, άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας εφημερίδας και να εισαγάγουν πρωτοσέλιδο ψευδές άρθρο για τον πρόωρο θάνατο του πρωθυπουργού, που εκείνη τη στιγμή νοσηλευόταν.

Διαθεσιμότητα (Availability) των δεδομένων και των υπολογιστικών πόρων - είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται.

Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DoS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας στοχευμένοι πόροι είτε προσωρινά, είτε μόνιμα, όχι κατ' ανάγκη από εχθρική επίθεση.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Ειδική Υπηρεσία Διαχείρισης
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή που ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωμάτωσε στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Ο κανονισμός 2016/679 της ΕΕ, την αντικαθιστά και θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης. | www.dpa.gr

Καλές Πρακτικές Χρήσης Email

- Αποφεύγουμε να ανοίγουμε συνημμένα αρχεία εκτός αν γνωρίζουμε τον αποστολέα ή/και είναι αναμενόμενα.
- Είμαστε προσεκτικοί σχετικά με τα μηνύματα e-mail που μας καθοδηγούν να ενεργοποιήσουμε μακροεντολές πριν από τη λήψη των συνημμένων Word ή Excel.
- Χρησιμοποιούμε λογισμικό προστασίας από ιούς στον υπολογιστή/laptop/tablet και βεβαιώνουμε ότι είναι ενημερωμένο με τους πιο πρόσφατους ορισμούς ιών.
- Μαθαίνουμε πώς να αναγνωρίζουμε τις τεχνικές υποκλοπής δεδομένων (phishing):
  - Μηνύματα που περιέχουν απειλές για το κλείσιμο λογαριασμού μας
  - Αιτήματα για προσωπικές πληροφορίες όπως κωδικοί πρόσβασης ή αριθμοί κοινωνικής ασφάλισης
  - Μηνύματα που περιέχουν λέξεις όπως «Επείγον», με ψευδή αίσθηση επείγουσας ανάγκης
  - «Ασυνήθιστες/’Υποπτες» διευθύνσεις email
  - Κακή διατύπωση της γλώσσας ή/και κακή γραμματική
- Τοποθετώντας το ποντίκι πάνω από τους συνδέσμους προτού κάνουμε κλικ σε κάποια διεύθυνση, βλέπουμε την διεύθυνση URL και διαπιστώνουμε σχετικά εύκολα εάν «φαίνεται ύποπτη».
- Δεν δίνουμε την διεύθυνσή του ηλεκτρονικού ταχυδρομείου σε ιστότοπους που δεν εμπιστευόμαστε και δεν εξυπηρετούν τα συμφέροντα του οργανισμού.
- Δεν δημοσιεύουμε τη διεύθυνσή του ηλεκτρονικού ταχυδρομείου μας σε δημόσιους ιστότοπους ή fora. Κακόβουλοι (spammers) σαρώνουν συχνά αυτούς τους ιστότοπους για διευθύνσεις ηλεκτρονικού ταχυδρομείου.
- Οι αξιόπιστες επιχειρήσεις δεν θα ζητήσουν ποτέ προσωπικές πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου.

Για παράδειγμα, οι τράπεζες δεν καλούν τους πελάτες τους ούτε στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου ζητώντας εμπιστευτικές πληροφορίες, όπως αριθμούς λογαριασμών, κωδικούς πρόσβασης, αριθμούς προσωπικής ταυτότητας (PIN), αριθμούς κοινωνικής ασφάλισης κ.λπ.

Κωδικοί Πρόσβασης

- Οι κωδικοί πρόσβασης, είναι προσωπικοί και θα πρέπει να τηρείται το απόρρητο. Προσοχή θα πρέπει να δίδεται στην αναγραφή τους σε σημεία τα οποία είναι προσβάσιμα και από άλλους πέραν του χρήστη.
- Αλλάζουμε τον κωδικό μας συχνά.
- Χρησιμοποούμε ισχυρούς κωδικούς πρόσβασης χρησιμοποιώντας συνδυαστικά αριθμούς, σύμβολα, πεζά και κεφαλαία γράμματα (*T3nd3r_1s_th3 N1ght*).
- Χρησιμοποιούμε ένα διαφορετικό κωδικό πρόσβασης για κάθε λογαριασμούς μας. Χρησιμοποιώντας τον ίδιο κωδικό πρόσβασης για τον τραπεζικό λογαριασμό όπως και για τον λογαριασμό ηλεκτρονικού ταχυδρομείου, γινόμαστε πολύ πιο ευάλωτοι στην κλοπή δεδομένων.

Οι κωδικοί πρόσβασης είναι σαν την οδοντόβουρτσα: επιλέγουμε το κατάλληλο, δεν το μοιραζόμαστε ποτέ, το αντικαθιστούμε με νέο τακτικά.

Καλές Πρακτικές στον Χώρο Εργασίες

Καθαρό γραφείο: γραφείο απαλλαγμένο από εταιρικά ή/και προσωπικά δεδομένα, πληροφοριακό υλικό, τα οποία έχουν απομακρυνθεί από το χώρο εργασίας. Η κατάλληλη ασφάλιση τους, περιορίζει την έκθεση / διαρροή στο χώρο εργασίας.

- Οποιεσδήποτε ευαίσθητες / εμπιστευτικές πληροφορίες αφαιρούνται από το γραφείο και ασφαλίζονται σε συρτάρι όταν το γραφείο είναι κενό, καθώς επίσης και στο τέλος της εργάσιμης ημέρας, αλλά και όταν αναμένεται να απουσιάσουμε για μεγάλο χρονικό διάστημα (άδεια).
- Ασφαλίζουμε τους υπολογιστές όπως προβλέπεται από τις εταιρικές διαδικασίες (passwords κλπ), όταν ο χώρος εργασίας είναι κενός.
- Κλείνουμε τους υπολογιστές εντελώς στο τέλος της εργάσιμης ημέρας.
- Αρχεία που περιέχουν ευαίσθητες / εμπιστευτικές πληροφορίες παραμένουν κλειστά και ασφαλισμένα, όταν δεν χρησιμοποιούνται ή όταν δεν παρακολουθούνται.
- Κλειδιά που χρησιμοποιούνται για την πρόσβαση σε ευαίσθητες / εμπιστευτικές πληροφορίες, δεν πρέπει να παραμένουν χωρίς επιτήρηση.
- Φορητοί υπολογιστές/Tablets/Κινητά ασφαλίζονται όταν δε χρησιμοποιούνται.
- Συσκευές μαζικής αποθήκευσης, όπως δίσκοι CD ROM, DVD ή USB, αντιμετωπίζονται ως ευαίσθητες και κατά συνέπεια, πρέπει να παραμένουν ασφαλείς σε κλειδωμένο συρτάρι.
- Εκτυπώσεις που περιέχουν ευαίσθητες / εμπιστευτικές πληροφορίες, απομακρύνονται άμεσα από τον εκτυπωτή, για να μην ληφθούν από λάθος άτομο.
- Απόρρητα και εμπιστευτικά έγγραφα καταστρέφονται στους καταστροφείς.
- Πίνακες που περιέχουν ευαίσθητες / εμπιστευτικές πληροφορίες καθαρίζονται.

(*) Δεδομένα & Πληροφορία: Η Πληροφορία είναι το αποτέλεσμα επεξεργασίας Δεδομένων.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Ειδική Υπηρεσία Διαχείρισης
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020